4.10 Risk Management (*Satisfies iCMM process area 13 criteria*)

4.10.1 Introduction

The Perform Risk Management process (Figure 4.1-10) provides an organized, systematic decision-making process to effectively deal with uncertainty in accomplishing program objectives. **Risk is defined as a future event or situation with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and an unfavorable consequence/impact to the successful accomplishment of the well-defined program goals if it occurs. Risk Management is an organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve project objectives.** A risk creates *risk exposure* for a project based on the combined effect of its likelihood and consequence. It is recommended that the process be applied at all levels, from small projects to large programs, and be applied continuously throughout the program's lifecycle, looking at all aspects of the program (see Figure 4.10-2). The extent and depth of application of this process should be governed by the outcome(s) being supported. In other words, what decisions are involved at a given point in the lifecycle, and what are the relevant risk factors to be addressed to support those decisions? The risks shall be managed in a way that they are capable of being "rolled up" from a project or several projects to a program. Risk rollup involves a review of the consequences/impacts from a higher (program) level. The risks to meeting the objectives or benefits of these projects or programs are typically known as programmatic risks, though the source of these risks may be external to the program itself. This process complies with the requirements of the integrated Capability Maturity Model (iCMM) (Process Area 13). It also satisfies Electronic Industries Alliance (EIA) 632 requirement 24 and EIA 731 Focus Areas 2.5-2 through 2.5-8.

Process:

Perform Risk Management

ID No.: 4.10 (iCMM PA 13)
Date: March 25, 2002
Revision Date: September 30, 2004

Next Higher Level Process:
Perform System Engineering

Process Owner:
System Engineering Council

Process Objective:
Identify and analyze the uncertainties of achieving program objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

Inputs

a) Integrated Program Plan (or Risk Management Plan)
b) Integrated Program Schedule
c) Requirements
d) Concerns/issues
e) Analysis criteria
f) External environmental forces
g) Technology
h) Constraints
i) FAA Policy
j) Corporate strategy and goals

Providers

a) ITP
b) EXT
c) RM
d) EXT, ITP, RM, FA, Syn, TS, IM, SpecEng, IA, CM, LCE, V&V
e) IA
f) EXT
g) EXT
h) Syn, CM, LCE
i) EXT
j) EXT

PROCESS TASKS

Beginning Boundary Task
Identify risk

- Analyze risk
- Select risk mitigation option
- Implement risk mitigation plan

Ending Boundary Task
Monitor and track risks

Lifecycle Phase

- ☑ Mission Analysis
- ☑ Investment Analysis
- ☑ Solution Implementation
- ☑ In-Service Management
- ☑ Service Life Ext.
- ☑ Disposal

Outputs

a) Program risk register
b) Risk mitigation plans
c) Risk mitigation plan summary
d) Program risk summary
e) Program risk mitigation progress
f) Constraints
g) Tools/analysis requirements
h) Planning Criteria

Customers

a) EXT
b) EXT, RM, Syn
c) EXT
d) EXT
e) EXT
f) FA, Syn, TS, SpecEng, V&V
g) IA
h) ITP

Figure 4.10-1. Risk Management Process-Based Management Chart

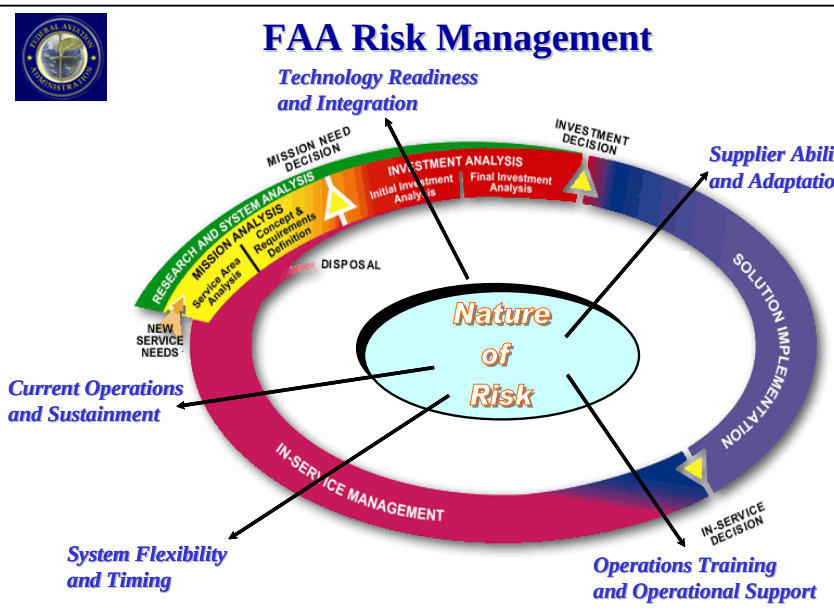


Figure 4.10-2. Risk Management Applied to All Program Aspects

4.10.1.1 Function of Risk Management

Risk management is a basic system engineering element of successful program management (Figure 4.10-3). When properly executed, Risk Management engages all disciplines and execution teams and is present in all program stages/phases. The functions (Figure 4.10-4) of the process are to:

- Identify each risk to the program
- Analyze and assess the negative consequences/impact and the likelihood/probability of the risk actually occurring and determine the risk realization date
- Develop specific approaches and plans to mitigate the risk
- Implement the risk-mitigation plan
- Monitor and track risk-mitigation effectiveness

Based on results from these functions, program management may then determine:

- The amount of schedule and budget reserves to be allocated and to what, based on identified risks
- How to measure overall program performance with respect to each risk
- How much and what type of help is needed from other sources
- When to look at the process to see if the mitigation effort is working

- When to add mitigation efforts, costs, and milestones to integrated program schedule and budget

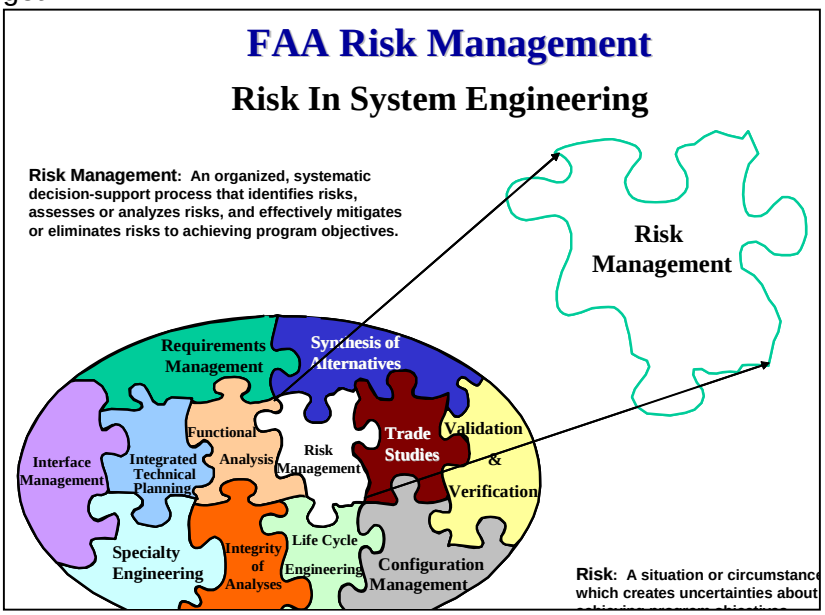


Figure 4.10-3. Risk in System Engineering

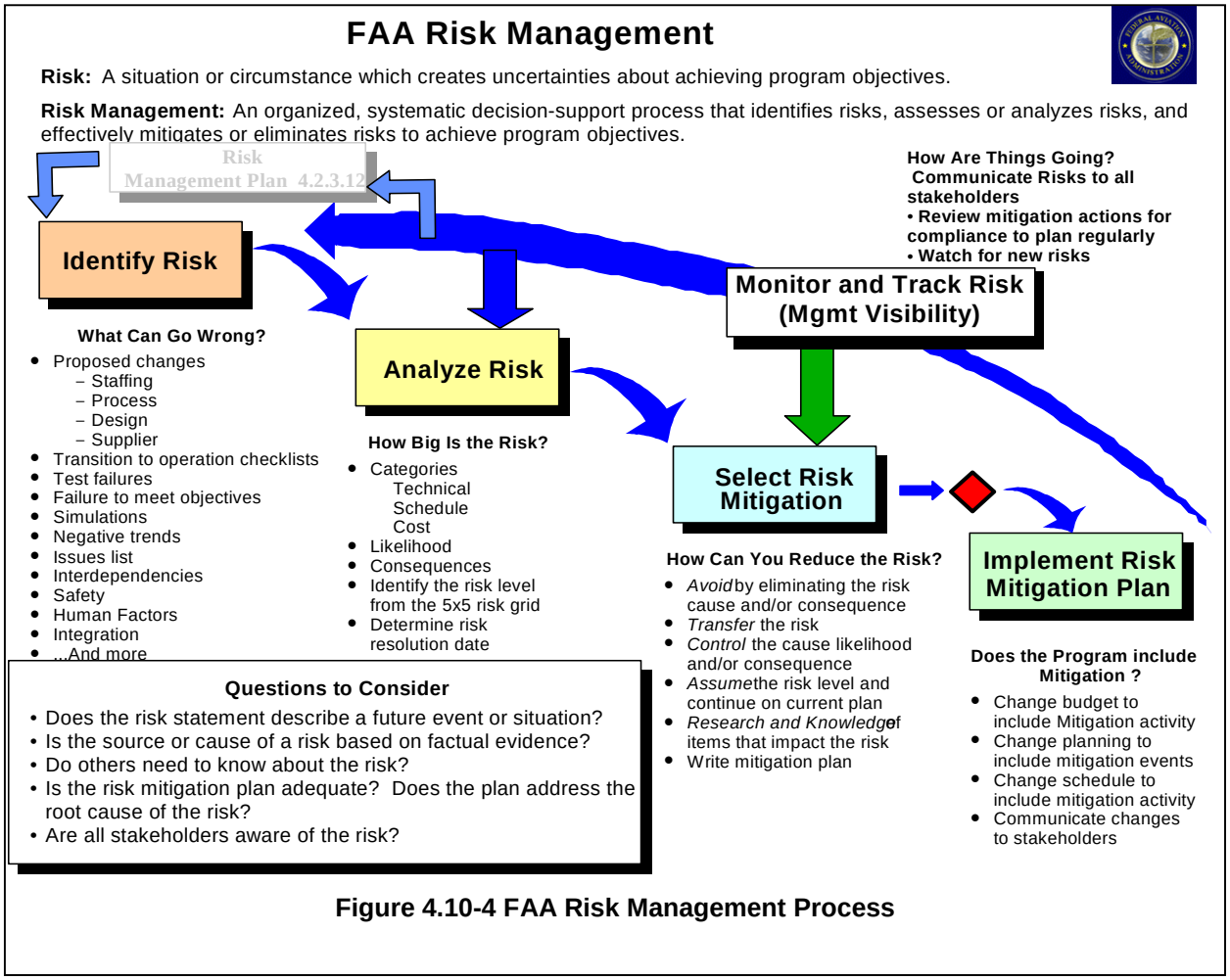


Figure 4.10-4 FAA Risk Management Process

4.10.1.2 Objectives of Risk Management

The fundamental objective of the Risk Management process is to identify and analyze uncertainties of achieving program objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

This process is applied to ensure that a program meets technical, schedule, and cost commitments; delivers a product that satisfies all stakeholders' lifecycle needs; and provides the expected benefit. Four lower-level objectives are established as part of the overall objective:

- Timely identification of risks (identifying a potential problem with sufficient leadtime so the team may implement appropriate alternate plans)
- Consistent assessment of the level of risk across a program (providing a structured decision-making framework for prioritizing resource application)
- Communication of risk-mitigation actions across the program/project (ensuring that all elements of the program/project are aligned in resolving risks)
- Review of risk-mitigation action performance

4.10.2 Process Description *(Satisfies iCMM PA-14, BP13.04 criteria)*

Every participant in a program/project shares the responsibility of assessing and mitigating risks. The process is a part of the overall program/project management and system engineering process. This process shall be aligned with the individual products (hardware, services, and software) that result from consistent functional analysis and requirements allocations, the Integrated Program Plan (IPP), the integrated program schedule, the associated funding, and the identified goals and benefits. The program is assessed as to risks associated with impacts on program benefits, interdependent programs, or environments. For each product, risks are evaluated against the acquisition baseline technical requirements, schedule, and cost leading to the successful satisfaction of the program objectives. Risks are identified, assessed, and appropriate risk-mitigation actions are established that comply with the program/project risk management plan within the IPP (see Section 4.2, Integrated Technical Planning, Paragraph 4.2.2.2). This plan is developed and tailored (when the technical nature of the program demands tailoring per Section 3.5) to satisfy the specific program/project needs. ***(Satisfies iCMM BP 13.01 criteria)***

Results from each assessment are a starting point for the risk-mitigation plan to support program management decisions (technical, schedule, and cost). The products of this process are also shared with stakeholders to achieve alignment/acceptance of the resource decisions. All risks are examined at each program/project/event/item/peer review as defined in the risk management plan. Updates reflect changes in risk resulting from planned mitigation activities or other unplanned events. Risk progress is actively tracked. For each risk, a "risk realization date" is established, marking the point in time when either the risk no longer exists or when the program shall be modified to accommodate the negative consequences. The question to be asked and answered is: "What happens on this date?" Risk is "rolled up" when it is taken from a lower-level project to a higher-level program or from a lower level organization to a higher one for review and mitigation.

An essential element of the Federal Aviation Administration (FAA) Risk Management process from an organizational point of view is the non-advocate concept. The purpose of a non-advocate is to provide an impartial, objective assessment of the project team's results, especially with respect to the assignment of risk levels. The input of a non-advocate is essential on those projects where two or more of the project specialists disagree on the risk levels. A non-advocate would typically be, but not be limited to, a program management person (above or at the same level of the program/project manager), a stakeholder representative, and/or a person from another project or program. The responsibility of a non-advocate is to examine and assess all aspects of the program/project risk management process before each review. For small projects, one or two non-advocates may be acceptable. A non-advocate provides an assessment to program/project managers for consideration and action.

4.10.2.1 Overview

The top-level process for Risk Management is shown in Figure 4.10-1. The process includes steps that result in identification of potential risks, analysis and assessment of risk, development of risk-mitigation plans, implementation of the Risk-Mitigation Plan, and monitoring of risk status. The process is iterative and is used across the program throughout the program's

Table 4.10-1 Risk Management and the AMS Lifecycle Phases

Risk Activity	R&D to Mission (1) Analysis	Initial Investment (2a) Analysis	Final Investment (2b) Analysis	Beyond IA
Risk Focus	**Assessment of operational risk associated with new concepts**	**Assessment of comparative risks between alternatives**	**Lifecycle risks of the selected alternative; Risk Management Plan for IPT**	**Program execution** **Acquisition Reviews**
Depth of Risk Assessment	**High-level**	**Some detail**	**More detailed**	**Detailed**
Risk Products	• **Identification of potential risks** • **General risks and requirements for any proposed alternative**	• **Comparative risk analysis for each alternative** • **Initial risk–adjusted cost and benefits baseline**	• **Updated Risk Analysis** • **Risk Management Plan (in IPP)** • **Final risk–adjusted cost and benefits APB**	• **Risk Management Plan** • **Risk Tracking Matrix** • **Etc.**
Risk Leadership Role	**Stakeholder/** **Organization**	**Investment Analysis Team**	**Investment Analysis Team**	**IPT/Sponsor/ System Operator**

lifecycle, with the nature of the risks changing to coincide with the lifecycle stage. The lifecycle dimension of Risk Management is illustrated in Table 4.10-1. Specific knowledge domains implement variants of this process to fit their specific needs and environment. However, all domains effectively perform Risk Management as shown in Figure 4.10-4.

4.10.2.2 Inputs

An expanded set of inputs capable of initiating Risk Management includes both program/project- and product-related data as shown in Table 4.10-2. Many of these inputs are developed and refined through the continuous, iterative use of other system engineering processes. Each table item is to be evaluated for resultant program risk (bolded items are shown in Figure 4.10-1 Process-Based Management Chart).

Table 4.10-2. Inputs to Risk Management

Input	Reference
Integrated Program Plan (or Risk Mgmt Plan)	4.2.1
System Engineering Management Plan (SEMP)	4.2.3.2
Integrated Safety Plan	4.2
Acquisition Strategy Paper	
Test plans	4.12
Integrated Program Schedule	
Requirements	4.3.3
Mission Need Statement and CONOPS	
Interfaces	4.7
Statement of Work	
Concerns/Issues	Appendix D
Trade Study Results	4.6.1.4
Design Analysis Results	4.8.4.3
Controlled Data and Reports	4.11.8
Specialty Engineering Analysis Results	4.8
Safety and/or Security Assessments	4.8
Human Factors Assessments	4.8
Verification Results	4.12
Training Results	
Maintenance Results	4.13
Operational Results	
Lessons Learned	
Program Review Results	4.2.6
Analysis Criteria	4.9.5.5
External Environmental Forces	
Acquisition Program Baseline (APB)	FAST
Acquisition Reviews	4.2.6
Contractor Outputs	
Technology	
Constraints	
NAS Architecture	4.5.5
Manufacturing/Production Information	
Product Configuration Data	4.11.3
Resources/Budgets	
FAA Policy	
AMS Documents	FAST
Corporate Strategy and Goals	
Contract	

4.10.3 Risk Management Process Tasks

The Risk Management process is summarized in Figure 4.10-1. The major process steps shown in Figure 4.10-4 are described in the remainder of this section.

4.10.3.1 Task 1: Identify Risk *(Satisfies iCMM BP 13.02 criteria*)

Risk identification is a systematic effort to uncover possible events or conditions that, if they occur, may hinder achievement of program objectives. The process begins concurrently with program or project planning and continues throughout the life of the program. While risk events or conditions may have many different root causes (e.g., equipment interoperability requirements, maintainability and supportability requirements, installation deadlines, contractual arrangements), the identification process isolates those events or conditions that may affect program technical performance, cost performance, or the program schedule. At the conclusion of the identification phase of risk management, it is recommended that a program manager have a list of (uncertain) events and conditions that may affect program cost, schedule, or technical performance. Risk identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status. Circumstances requiring assessment for potential risks include:

- Programmatic changes
- Unfavorable trends in Technical Performance Measures, predicted system performance, schedules, and financial status
- Design/Program/Peer reviews
- Change proposals (including proposed changes in requirements)
- Occurrence of a major unforeseen event
- Newly identified risks
- Special assessments at the direction of Agency Management
- Changes or risks in interdependent programs
- Environment changes

As shown in Figure 4.10-5, participants in risk identification include all stakeholders, users, suppliers, and appropriate members of execution teams. Teams consider all likely risk sources in identifying potential risks to the program/project. Risk identification is based on the current program/project goals supported by the associated technical, schedule, and cost requirements and plans.

A risk has three aspects: (1) the likelihood/probability that an event will occur (a degree of uncertainty), (2) the event is in the future, and (3) an unfavorable consequence/impact if it occurs. It is recommended that the likelihood of a risk occurring not be so low as to be negligible (i.e., probability essentially equal to zero) nor be equal to 1, which typically indicates that it has, in fact, already been realized. A risk shall also have a negative consequence/impact if realized. Positive consequences are not considered in the FAA risk identification and analysis

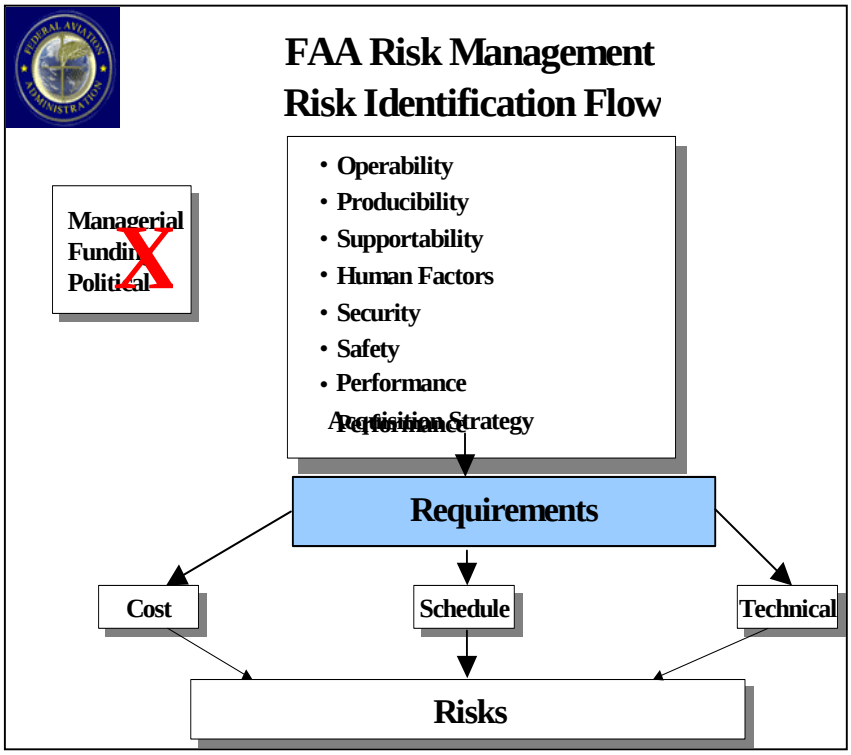


Figure 4.10-5. Risk Identification Flow

process; these are considered opportunities. Note that if there is no uncertainty (i.e., the situation or circumstance is certain to occur or has already occurred), there is no risk even though the item has an unfavorable consequence. It is recommended that this situation be handled as a management issue or concern, for which a corrective action plan shall be generated and implemented. This essentially requires rebaselining the program or possibly canceling the program if the negative consequences are too severe.

Each risk shall have a "risk realization date." This is a date when either the risk no longer exists or when the program shall be modified to accommodate the negative consequences. This date shall be documented when the risk is identified. The question to be asked and answered is: "What happens on this date?" The negative consequence of the outcome of the event that occurs on a given date is the basis for the risk.

4.10.3.1.1 Potential Sources of Risk

Risks originate from three basic areas—technical (or performance), schedule, and cost. A risk identification flow is shown in Figure 4.10-5. Technical risk is based on the likelihood that the program as planned will be unable to deliver a product to satisfy the technical requirements. As such, well-documented, defined and quantified technical requirements are necessary to define a technical risk. Most of the risks listed in Table 4.10-2 are technical risks. Schedule risk results from the likelihood that the program actions may not be accomplished in the planned program timing. A detailed program schedule identifying each accomplishment and the critical path is necessary to develop schedule risks. Cost risk results from the likelihood that the program may not accomplish planned tasks within the planned budget. A detailed budget, in which the cost of each accomplishment is specified and any management reserve is known, is needed to determine a cost risk. Potential loss of funding is typically not a program risk in this risk process

because the funding decision is made at the Agency level, and the financial risk to the program occurs once a decision has been made to allocate the existing Agency funding among programs and/or organizations. Within the FAA risk process, ***cost*** is the ultimate expenditure required for a resource and the end product produced by that resource. ***Budget*** is the forecast of all costs planned for a given project/program, and ***funding*** is the supply of money provided to accomplish a given project/program. The risk source is based on the **root cause** of the risk and, as such, only a single source will cause a risk. The source is either technical, schedule, or cost in nature and not a combination or all of these. This is not to be confused with the symptoms, which may manifest themselves as some combination of performance (technical), benefit, cost, and/or schedule impact.

A program's acquisition strategy generates risks in its own right. Development programs are different in nature from those using commercial-off-the-shelf (COTS) solutions. Risks that need to be considered in a COTS-based acquisition appear in Figure 4-10.6.

For each risk area, it is recommended that many sources be considered. For technical risk, likely sources include technology maturity, complexity, dependency, stakeholder uncertainty, requirements uncertainty, and testing/verification failure. Sources of schedule risks may include incomplete identification of tasks, time-based schedule (as opposed to event-based schedule), critical-path scheduling anomalies, competitive optimism, unrealistic requirements, and material availability shortfalls. Cost risks may stem from an uncertain number of production units, supplier optimism, additional complexity, change in economic conditions, competitive environment, supplier viability, and lack of applicable historical data.

Table 4.10-2 provides the potential sources of risk that shall be considered in the process of program risk assessment. This listing provides an excellent starting point for identifying potential risk areas when combined with the input factors shown in Table 4.10-1.

Table 4.10-2. Potential Sources of Risk

Potential Sources of Risk	
• Safety • Security • Maintainability • Reliability • Supportability • Human Factors • Availability • Decommissioning • Reducibility • Commonality • Training • Operations	• Test • Verification • System Integration • Staffing • Tools • System Performance • Technology • Planning • Transition • Environments • Interdependencies (both FAA and non-FAA) • Acquisition Strategy

COTS Considerations

Number	*COTS Risk Factor (Characteristic)*
01	COTS products can exhibit rapid and asynchronous changes.
02	COTS product obsolescence can affect systems in different ways.
03	COTS products are typically documented with proprietary data.
04	Low initial costs of COTS products can be offset by higher lifecycle costs.
05	Functionally equivalent COTS products/systems can have multiple configurations
06	Different COTS product vendors have different quality practices.
07	COTS products form, fit, and function are sold "as is."
08	COTS products are developed to commercial standards.
09	COTS products typically have time-limited manufacturer support.
10	COTS product inter-operability can introduce information security susceptibility.

Figure 4.10-6. COTS-Based Risk Considerations

The knowledge domains of safety and security impose additional criteria or gates as part of their identification process. In the case of safety, the process commences with an analysis, which identifies potential hazards that are the basis for identifying safety related risks. Safety does not identify a risk until a hazardous situation has been identified.

Information security engineering also utilizes a series of gates prior to identifying a risk. Security is concerned about the existence of viable threats, which may exploit a system vulnerability to cause harm. The combination of a viable threat coupled with a vulnerability in the system that is capable of being exploited by the threat is necessary before the security community moves to declare a (security) risk.

4.10.3.1.2 Risk Identification Methods

Risk identification begins at the lowest feasible level and normally includes inputs from all stakeholders and suppliers. Anyone may identify a potential risk. It is recommended that experts review programs to determine that risks related to their domain(s) have been completely identified. It is also recommended that similar programs be reviewed for determined risks as well as actual problems. The objective of this step is to produce as comprehensive a list as possible of potential risks. This may be achieved using any combination of methods, such as group discussions, interviews, trend/failure analysis, risk templates, lessons learned, trade studies, Best Practices, metrics, and acquisition documentation. It is recommended that the focus be on root causes and not on symptoms of a more basic problem. The problem shall be defined at the lowest level (root cause) so that the mitigation plan actually addresses the problem.

This process includes screening the list of risks for duplication and consolidation as appropriate. Program Management errors are not risks and shall be corrected before the program moves forward. It is recommended that this screening consider program-level ramifications and ensure that program integration risks are adequately covered. A Risk Worksheet (Figure 4.10-7) may be used to document newly identified potential risks.

4.10.3.2 Task 2: Analyze and Assess Impacts of Risk *(Satisfies iCMM BP 13.03 criteria)*

Risk analysis or risk assessment provides program insight into the significance of identified risks. Risk analysis attempts to assess the likelihood of identified risks and the consequence to the program if the risk event or condition occurs. The process also classifies each risk according to the root cause of the risk event (cost, schedule, or technical performance).

Risk analysis assesses each component of an identified risk: (1) the likelihood of the risk occurring, and (2) the consequence to the program if it occurs, as depicted in Figure 4.10-8. The basic tool used for qualitative risk analysis is the risk template, which contains a set of definitions to be used to evaluate the likelihood and consequence of a particular risk. The set of templates that a program uses may change over time as new templates are added or existing templates are changed, combined, or eliminated. The program may choose to use program-unique templates (only if the technical elements of the program demand it), which are based on and traceable to program or stakeholder requirements, provided supporting rationale is given. However, modification of templates limits the ability to “roll-up” risks to a higher program level, and, as such, a mechanism shall be developed to correlate risks developed through modified templates to the risks developed with the standard FAA templates. The program/project is responsible for the choice, coordination, and control of the templates used on the program. These decisions are contained in the Risk Management Plan section of the SEMP (see Paragraph 4.2.3.12 in Integrated Technical Planning (Section 4.2)).

The result of the risk analysis process is an assignment of a measure termed risk exposure to each identified risk. Risk exposure is one quantitative figure of merit that represents the combined effects of likelihood and consequence; it serves as an aid to program management in ranking identified risks from most severe to least severe. At the conclusion of the risk analysis process, it is recommended that program management have visibility into the range of possible outcomes for the program (in terms of achieving objectives) if in fact an identified risk event or condition occurs.

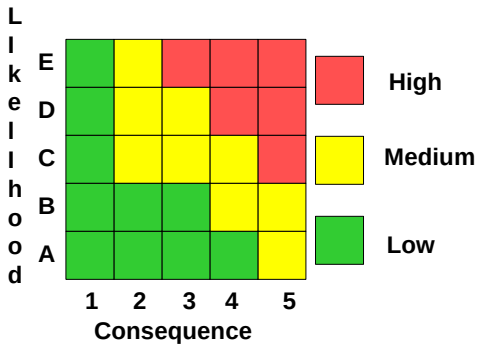
FAA Risk Worksheet

Program/Project Title_____ **Seq. #:** _____

Submitted by: _____ **Date:** _____

Risk:	**Point of Contact**
Source and Root Cause:	

	Risk Assessment			**Rationale**
o	**Technical**	o **Schedule**	o **Cost**	
	Likelihood	A B C D E		
	Consequence	1 2 3 4 5		



Consequence Definition:

Risk Realization Date:

5	**Mitigation Options**	Description	New Risk Level if Implemented
☐	**Avoidance**		H M L
☐	**Transfer**		H M L
☐	**Control**		H M L
☐	**Assumption**		H M L
☐	**Research & Knowledge**		H M L

Submitted: _____ **Date:** _____	☐ **Mitigation Approved**	☐ **Disapproved**
Approval: _____ **Date:** _____	☐ **Approved w/ Change**	☐ **Returned**
	☐ **Risk Accepted**	☐ **Closed**

Figure 4.10-7

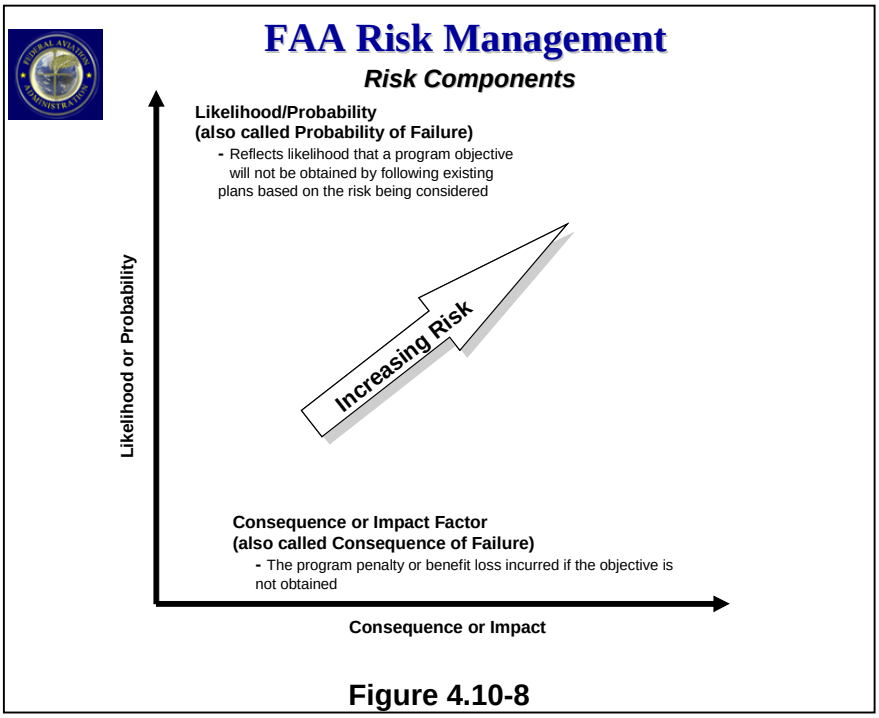


Figure 4.10-8

4.10.3.2.1 Likelihood (Probability) Determination

A likelihood (probability) template is developed that applies to the specific risk/program under analysis. A new template is developed and documented if none of the existing program templates are found to be applicable. This action shall be coordinated within the program/project using the criteria of the Risk Management Plan. Correlation of the new templates to the standard FAA templates in this manual shall be established. Figure 4.10-9 provides the FAA definitions of the risk likelihood levels.

4.10.3.2.2 Consequence Determinations

Another set of templates is used to evaluate consequence/impact to the program if the risk materializes. Consequence templates are shown for three areas of program impact: technical (Figure 4.10-10), schedule (Figure 4.10-11), and cost (Figure 4.10-12). The choice of the consequence template to be used to evaluate a given risk is determined by the nature of the root cause of that risk. If the root cause is technical in nature, it is then recommended that the technical consequences template be used. It shall be remembered that each of these results in a risk, which threatens the benefits of a program and may also have interdependency impacts. The symptoms of the risk may materialize in any combination of program areas: technical (or performance), schedule, and/or cost. However, treating the symptoms only wastes program resources and does NOT directly deal with the source or root cause of the risk.

All NAS programs are developed to provide benefit(s) to the system. Risk ultimately reflects in impacts to benefit(s). All benefit losses are derived from negative impacts in either technical, schedule, or cost risks. This is a significant part of the risk consequence that shall be defined. The cost/benefit analysis shall be reexamined as a result of risk-driven impacts to provide the information needed to make program decisions. As was the case with likelihood templates, if none of the existing program consequence templates are found to be applicable to a particular risk, new templates may be developed and documented. Correlation of the new templates to the standard FAA templates in this manual shall be established.

FAA Risk Likelihood Definitions

What is the likelihood the risk will happen?

A. **Not Likely**: Your approach and processes will effectively avoid or mitigate this risk based on standard practices (<10% chance it **WILL** occur).

The chance of a negative outcome based on existing plans is not likely. This likelihood level assessment should be based on evidence or previous experience and not on subjective confidence. This assessment level requires the approach and processes to be well understood and documented. Little or no management oversight will be required.

B. **Low**: Your approach and processes have usually mitigated this type of risk with minimal oversight in similar cases (<1/3 chance that it **WILL** occur).

There is a low likelihood but reasonable probability that a negative outcome is possible. Present plans include adequate margins (technical, schedule, or cost) to handle typical problems. This assessment level requires the approach and processes to be well understood and documented. Limited management oversight will be required.

C. **Likely**: Your approach and processes may mitigate this risk, but workarounds will be required (~50% chance that it **WILL** happen).

A negative outcome is likely, or the current approach and processes are only partially documented. Alternative plans or methods exist to achieve an acceptable outcome even if the risk is realized. Present plans include adequate margins (technical, schedule, or cost) to implement the workarounds or alternatives to overcome typical problems. Significant management oversight will be required.

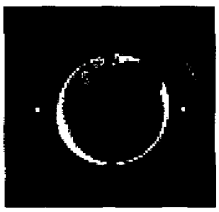
D. **Highly Likely**: Your approach and processes cannot mitigate this risk, but a different approach might (>2/3 chance that it **WILL** happen).

A negative outcome is highly likely to occur, or the current approach and processes are not documented. While alternative plans or methods are believed to exist to achieve an acceptable outcome, there are not adequate margins (technical, schedule, or cost) to implement the workarounds without impacting the program management reserves in performance, schedule, or cost. Significant management involvement is required.

E. **Nearly Certain**: Your approach and processes cannot mitigate this type of risk; no known processes or workarounds are available (>90% chance that it **WILL** happen).

A negative outcome is going to occur with near certainty. No alternative plans or methods have been documented. Alternatively, the risk item has yet to be evaluated adequately to be well understood, so there is a high level of uncertainty about the program success. Urgent management involvement is required

Figure 4.10-9



FAA Technical Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on system performance?

1. Low: Given that the risk is realized, there would be minimal impact.

   A successful outcome is not dependent on this issue; the technical performance goals will be met. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, there would be a minor performance shortfall but the same approach could be retained.

   The resulting technical performance would be below the goal but within acceptable limits. There would be no need to change the basic design, process, or approach. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a moderate performance shortfall but workarounds would be available.

   The resulting technical performance would be below the goal. The basic design, process, or approach could be retained with only minor changes, and the overall system performance would still be acceptable as a result of workarounds such as the reallocation of functions or performance goals. There would be only a limited impact on the success of the program.

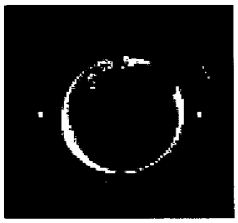
4. Significant: Given that the risk is realized, the performance would be unacceptable but workarounds would be available.

   The resulting technical performance would be unacceptably below the goal. The design, process, or approach would require a significant change to achieve an acceptable performance level. Additional workarounds such as the reallocation of functions or performance goals could also be required. The success of the program could be jeopardized.

5. High: Given that the risk is realized, the performance would be unacceptable with no known workarounds.

   The resulting technical performance would be unacceptably below the goal. There are no known alternatives or solutions. The success of the program would be in doubt.

Figure 4.10-10



FAA Schedule Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on the schedule?

1. Low: Given that the risk is realized, there would be minimal impact.

   The program schedule is not dependent on this issue. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, additional activities would be required to meet key dates.

   One or more key dates in the program schedule, but not critical path events, would be jeopardized; there are identified schedule workarounds that would be sufficient to mitigate the schedule impact. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a minor schedule slip, and one or more need dates would be missed.

   One or more key need dates in the program schedule, but not critical path events, would be at least one month late; there are identified schedule workarounds that would be sufficient to keep the program critical path from being affected. There would be only a limited impact on the success of the program.

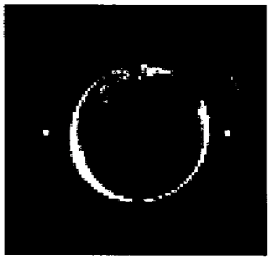
4. Significant: Given that the risk is realized, the program critical path would be affected.

   One or more events on the program critical path would be at least one month late. There are identified schedule workarounds that would be sufficient to meet major program milestones. The success of the program could be jeopardized.

5. High: Given that the risk is realized, a key program milestone cannot be achieved.

   Completion of a key program milestone would be late, and the success of the program would be in doubt. The slip requires a re-baseline of the program.

Figure 4.10-11



FAA Cost Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on cost?

1. Low: Given that the risk is realized, there would be minimal cost impact.

   Program cost is not dependent on this issue. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by = 1%.

   The program costs and/or the production unit cost would increase by = 1%. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a minor increase in financial need. The program costs, operating cost or unit production cost could increase above 1% up to = 5%.

   The program costs and/or the production unit cost would increase above 1% to = 5%. There would be only a limited impact on the success of the program.

4. Significant: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by above 5% to = 10%.

   The program costs and/or the production unit cost would increase above 5% to = 10%. The success of the program could be jeopardized.

5. High: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by greater than 10%.

   The program costs and/or the production unit cost would increase by greater than 10%. The success of the program would be in doubt.

Figure 4.10-12

4.10.3.2.3 Risk-Level Determination

The likelihood and consequence are considered to be independent, but tied to the same event, and are mapped into a risk grid to determine the individual risk level (e.g., high (red), medium (yellow), or low (green)) as shown in Figure 4.10-13. This mapping facilitates the prioritization and trend analyses of risks throughout the life of the program. Use of a "color code" for each

Risk-level definition high (red) is likely (a high probability) to cause significant disruption of

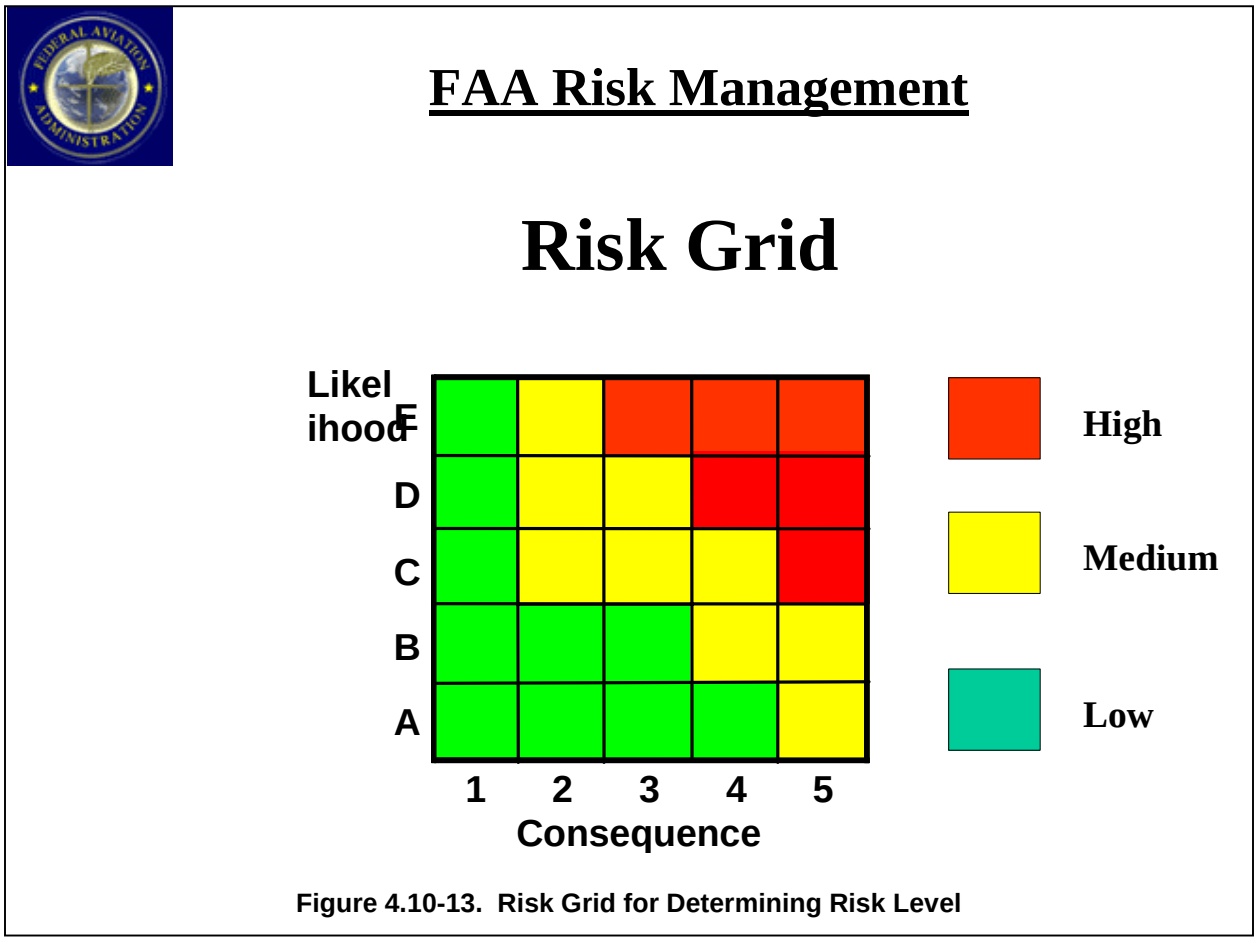


Figure 4.10-13. Risk Grid for Determining Risk Level

schedule, increase in cost, or degradation of performance. Concerted and continual emphasis and coordination may not be sufficient to overcome major difficulties. Medium (yellow) may cause some disruption of schedule, increase in cost, or degradation of performance. Special emphasis and close coordination is probably sufficient to overcome difficulties. Low (green) has little potential for disruption of schedule, increase in cost, or degradation of performance. Normal emphasis and coordination is probably sufficient to overcome difficulties. The threshold for differentiating between high, medium, and low may change from program to program, but not risk level supports effective communication of program health internally and externally for risk to risk, and it is recommended that it be determined early in the life of the program.

The color coding on this grid is also used to communicate management's threshold of risk acceptability. For acquisition or development programs, this threshold is usually the line between green and yellow. While development programs are focused on maturing a point

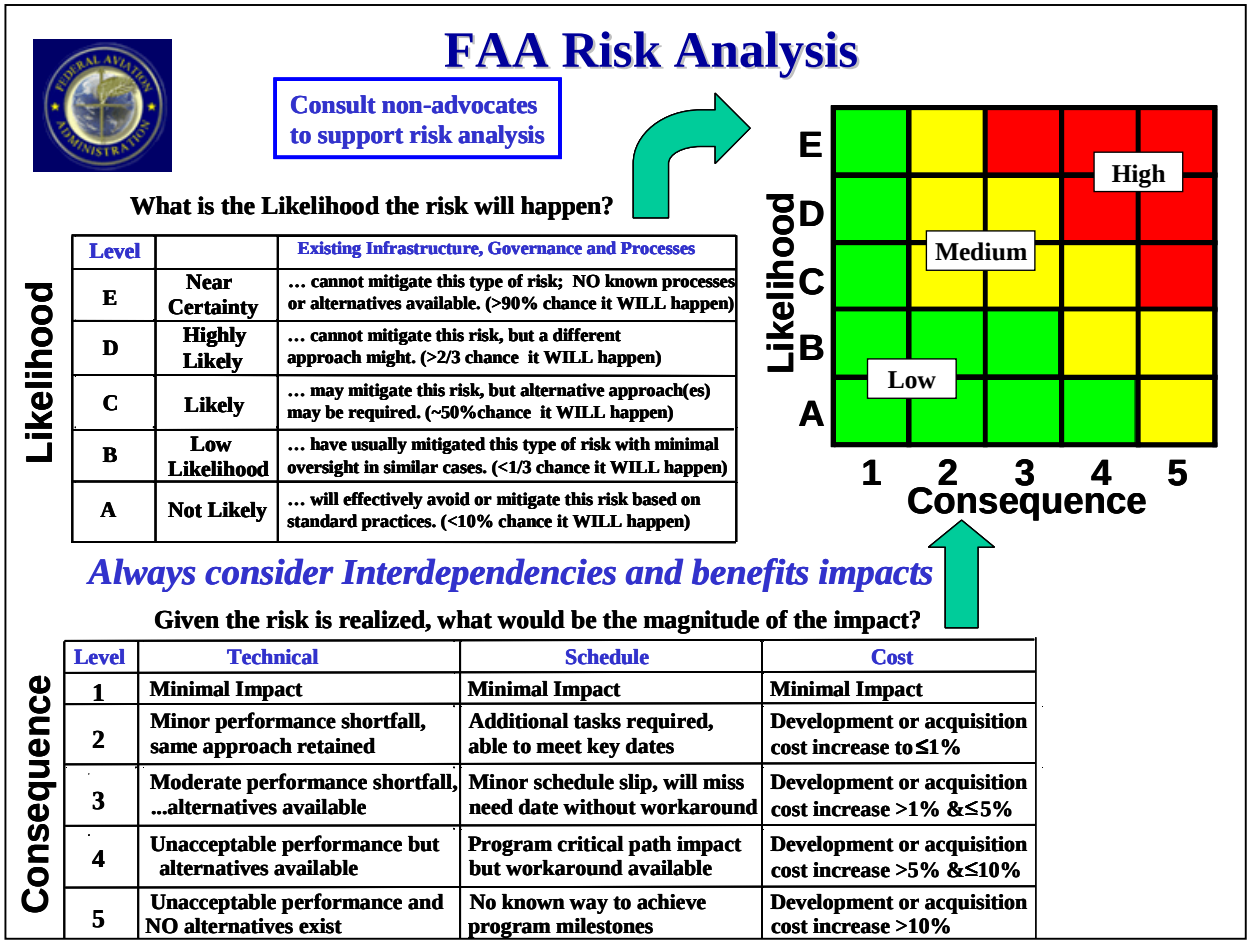


Figure 4.10-14. Risk Analysis

solution for a requirements set, research is aimed at determining the feasibility of an approach or technology. For research programs, the level of acceptability is typically defined as the threshold between yellow and red because the success criteria of research do not require the same degree of granularity as development. The degree of risk-level acceptance and the actions required to reduce a risk below that level shall be detailed in the Risk Management Plan. Figure 4.10-14 is a summary of how the consequence and likelihood are consolidated to define the risk level.

Various technical communities employ risk analysis techniques or methodologies specific to their domain. They portray their conclusions and recommendations as grids similar to that shown in Figure 4.10-14; but the scales vary from 3 x 3 to 10 x 10 with many variations in between. It is recommended that the representation a given specialty community (such as Safety or Information Security) uses to draw conclusions be suited to its particular situation. However, the criteria used and portrayal of a community's conclusions and/or recommendations shall be consistent with the program view of risk. Figure 4.10-15 illustrates this correlation for the ISE risk elements shown in Figure 4.8.6-5 (see Section 4.8.6, Information Security) and the basic risk elements discussed in this section. Regardless of the steps/methodologies used by a specialty knowledge domain, all risks need to be portrayed to management on the same basis

(see Section 4.10.3.5 below) to allow for effective decisions on the application of risk-reduction resources. However, the basic conclusion(s) reached by the specialty community must be preserved in any translation into a common program reporting format.

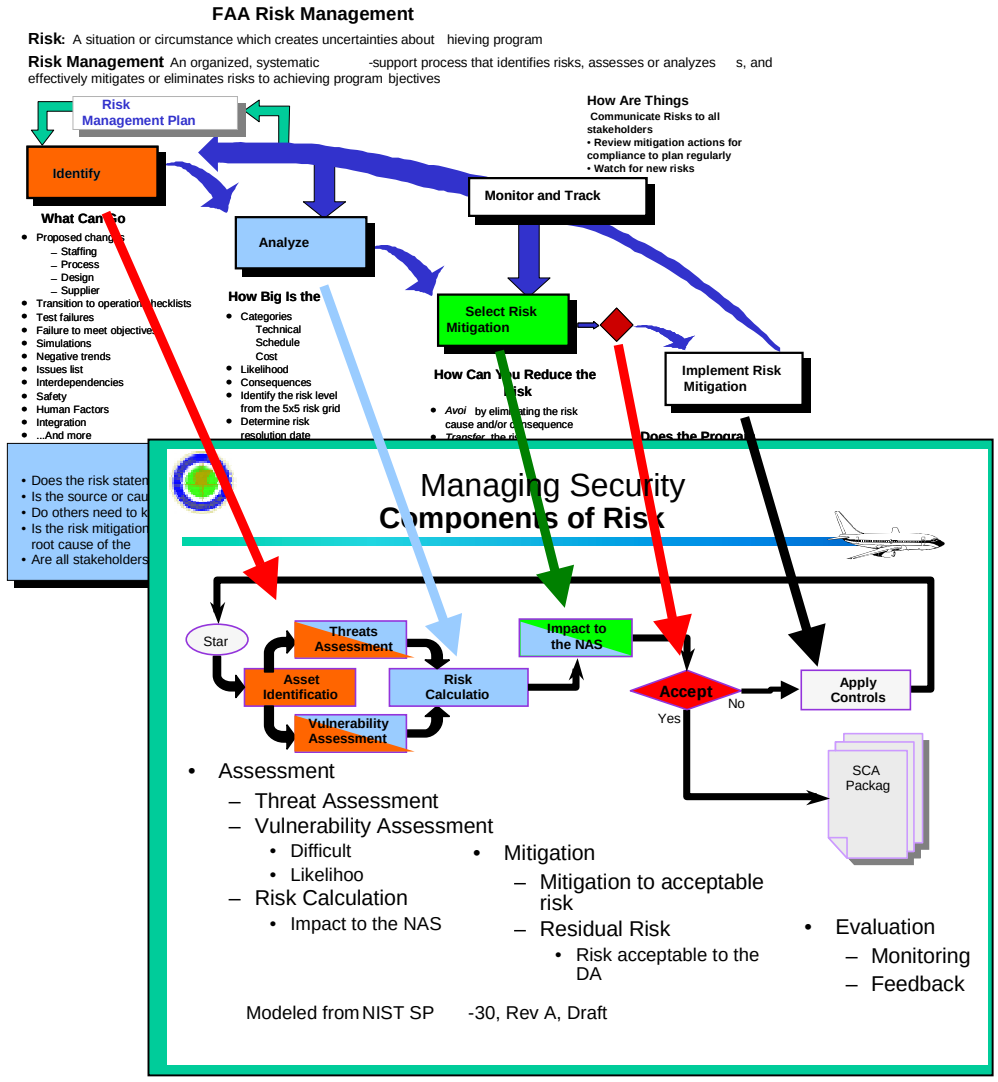
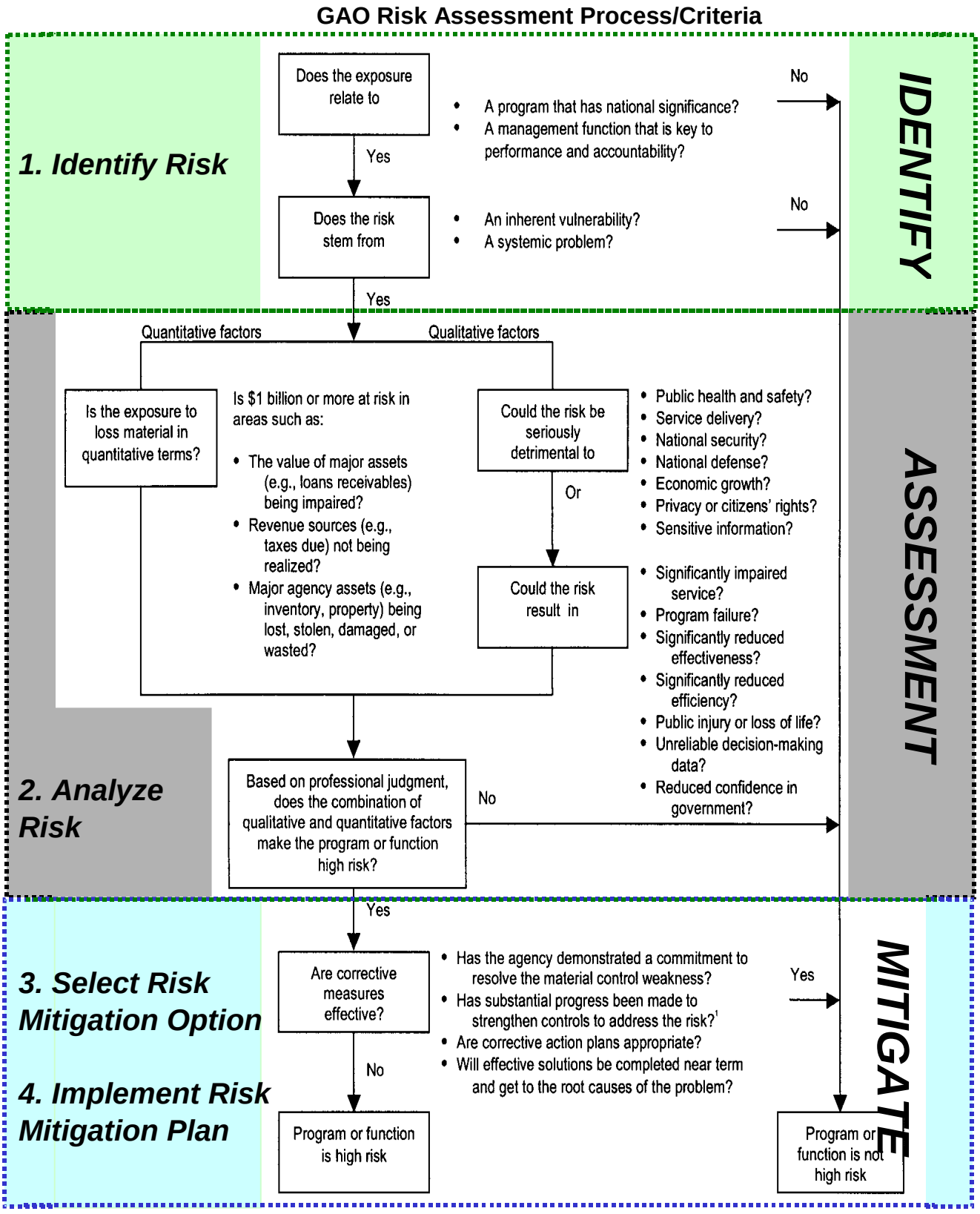


Figure 4.10-15. Correlation of Risk Management with Information Security Methodology

The General Accounting Office (GAO) has also defined a process to handle risk in a report issued in 2000 (Reference 16). It contains the same elements shown in the FAA Risk model with the exception of the track and control step. Figure 4.10-16 shows the correlation between the two approaches and demonstrates how the GAO recommendations are satisfied with the process described in the FAA System Engineering Manual (SEM).

FAA Risk Management



GAO process requires examination of risk and the development of a mitigation effort. Shown is Figure 5 of GAO/OCG-00-12, Page 9. (August/2000).

Figure 4.10-16. Correlation of GAO recommendations with FAA Risk Management

4.10.3.3 Task 3: Select Risk-Mitigation Option *(Satisfies iCMM BP 13.05 criteria)*

The objective of risk-mitigation handling is to implement appropriate and cost-effective risk-mitigation plans to mitigate or eliminate the risks. Appropriate risk-mitigation techniques are selected and mitigation actions are developed, documented, and implemented. Risk-mitigation handling (planning, implementation, and tracking) is the core of risk management. Risk-mitigation implementation requires a conscious management decision to approve, fund, schedule, and implement one or more risk-mitigation actions. Risk-mitigation plans and mitigation actions are reviewed frequently at major reviews, program reviews, acquisition reviews, and milestone reviews.

Risk-mitigation actions fall into one, or a combination, of the following strategies:

- Avoidance
- Transfer
- Control
- Assumption
- Research and Knowledge

"Avoidance" is a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the program. This technique may be pursued when multiple designs or programmatic options are available. It is more likely used as the basis for a "Go"/"No-Go" decision at the start of a program. Some examples are selection of state-of-the-practice rather than state-of-the-art technologies and prequalification of suppliers. The avoidance of risk is from the perspective of the overall program/project, which includes the stakeholders, contractors, and execution groups. Thus, an avoidance strategy is one that involves all of the major parties to the program/project and permits a program/project-wide avoidance of the risk.

"Transfer" is a strategy to shift the risk to another area, such as another requirement, an organization, a supplier, or a stakeholder. Examples include reallocating requirements, securing supplier product warranties, and negotiating fixed-price contracts with suppliers. Note that at the program level, the risk remains. The transfer of the risk is accomplished primarily to optimize, in a sense, the overall program risk and to assign ownership to the party most capable of reducing the risk. It is possible that the risk level may change as a result of the risk transfer.

"Control" is a strategy of developing options and alternatives and taking actions that lower or eliminate the risk. Examples include new concepts, more analysis, redundant systems and/or components, and alternate sources of production.

"Assumption" is simply accepting the likelihood/probability and the consequences/impacts associated with a risk's occurrence. Assumption is usually limited to low risks. This is a program/senior management option, not a project option. FAA practice is to develop mitigation plans for all medium and high risks.

"Research and Knowledge" may mitigate risk through expanding research and experience. Since risk arises from uncertainty and inexperience, it may be possible to effectively mitigate risk simply by enlarging the knowledge pool, leading to reassessment that reduces the likelihood of failure or provides insight into how to lessen the consequences.

At this point, several alternatives for mitigating the risk have been identified and analyzed for selection of the preferred approach. Alternatives include detailed plans for mitigating the risk in several small, sequential steps; alternative steps; or entirely new (nonbaselined) approaches to accomplishing the program. Further, contingency plans are identifiable alternatives, which may be implemented if a mitigation plan fails, and the risky event or conditions occur with more serious consequences than anticipated. The mitigation steps are the major milestones of the mitigation plan. Contingency plans need not be extremely detailed.

For instance, the risks associated with selecting a COTS-based acquisition approach (see Figure 4.10-6) have known risk-mitigation strategies. These strategies need to be included in the trade studies when comparing acquisition approaches. Because COTS has an inherent set of risks that are market-driven, most of the risk-mitigation strategies fall into the "Control" category in order to anticipate and reduce the risks to acceptable levels. More information on COTS risks and mitigation strategies may be found in the FAA COTS Risk Mitigation Guide, which is available at http://www.faa.gov/aua/resources/COTS.

Trade study techniques may be performed to help select the preferred risk-mitigation plan. While the proper criteria and their weights for each analysis are dependent on the risks to be mitigated, it is recommended that the following be included:

- Does the option mitigate the likelihood or consequence of the risk?
- Does the option fit within program scope?
- Is the option easy to implement?
- Are new risks avoided or introduced?
- What is the cost of mitigation?
- What is the schedule for mitigation?

The risk level is the first criterion used to determine the need for a risk-mitigation plan. Program risks that fall into the medium or high categories require risk-mitigation plans. Risks that are assessed as low typically do not require mitigation plans but may have certain aspects that would be prudent to monitor. If this is the case, risk-mitigation plans may be formally or informally implemented for these low-risk issues based on the specific Risk Management Plan for a program.

It is essential that those responsible for plan implementation have a thorough understanding of the risk to be mitigated. This may be accomplished with a good summary statement of the risk. It is recommended that the statement include descriptions of the future event or condition, which confirms trouble for the program; the root cause(s) of the event outcome or conditions; and the specific effects to the program if the event or conditions occur with negative consequences. It is recommended that the risk not be stated in terms of its mitigation plan.

It is recommended that the status also include a summary of risk-mitigation efforts that references more detailed documentation. A Risk Mitigation Plan Summary (Figure 4.10-17) is used to report the analysis and actions on an individual risk.

The risk-mitigation plan documents the specific steps to be implemented, the sequence in which they are to be implemented, and the points in time at which they are to be implemented. Developing a risk-mitigation plan includes assessing the expected outcome following implementation. It is recommended that the same method initially used to assess the risk, such as risk templates, be used to provide a forecast of the risk level after completion of each action of the risk-mitigation plan. The expected impact of each mitigation event on risk level may be projected using a format similar to that of Figure 4.10-18 (a "waterfall chart").

Risk ID No: AND490-001 Page 1 of 6

Risk Mitigation Plan Summary

Sample

Date: 04/15/3032 Status: Active

Risk Title: Scan rate low

Program/Project: ASR-27

Project Lead: Mr. Solo

Description of Risk
The scan rate of the radar sail may fall below the allowable tolerance

Statement of Root Cause
Analytical projections of motor power available may have overestimated power resulting assumption that requirements could be satisfied.

Consequence if Realized **Low scan rate provides inadequate data rate to remote control function resulting in increased approach separation and increased delays**

Risk Type: T S C
Likelihood D
Consequence 3
Comments:
Risk Resolution Date: 10/17/32

Place X in One Cell

Likelihood \ Consequence	1	2	3	4	5
E					
D			X		
C					
B					
A					

Risk Mitigation

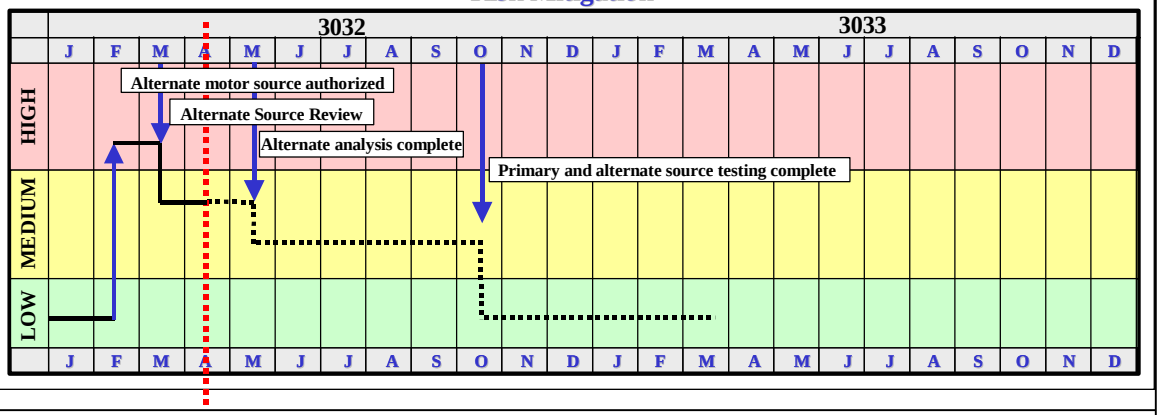


Figure 4.10-17. FAA Risk Mitigation Summary (Example)

Risk Mitigation Waterfall Schedule

Sample

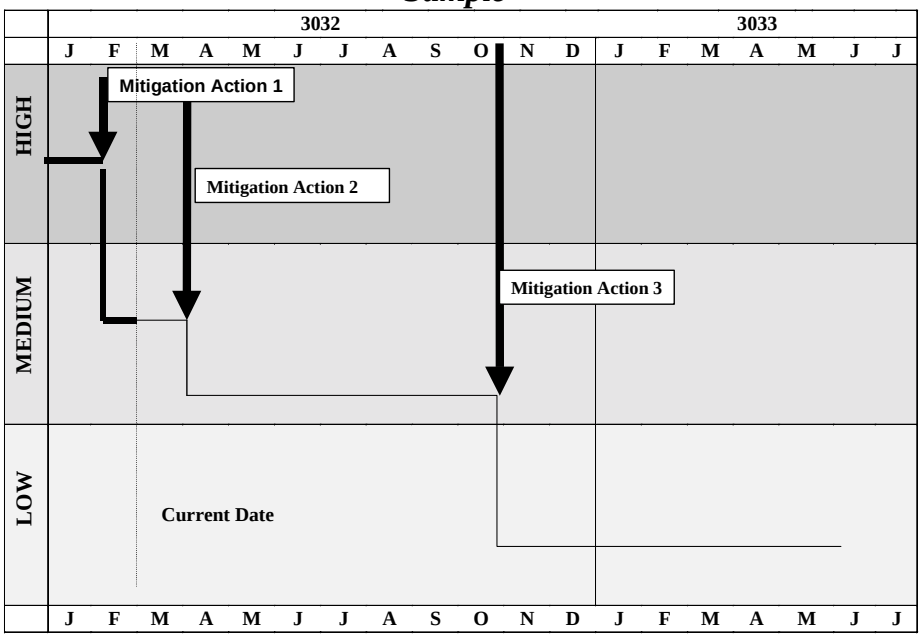


Figure 4.10-18. Typical Risk Mitigation Portrayal

The risk-mitigation plan becomes the basis for monitoring the success in mitigating each risk. The plan includes, but is not limited to, the following:

- A description of the risk for which the plan applies
- The mitigation approaches, which detail the specific actions that are planned to reduce the risk or eliminate it. It is recommended that these actions be event-based, integrated into a schedule, and have associated with each of them:
  - The decision point or trigger, past or future, that initiates the action or group of actions
  - The resources required to execute the actions (including personnel, capital equipment, facilities, procured equipment)
  - The measures of success to be used for the planned actions or group of actions
  - The fall-back options or contingency plans (if any)
  - The planned completion dates of the actions
- Risk-mitigation metrics
- The Risk Worksheet (Figure 4.10-7)
- The initial Risk Mitigation Plan Summary (Figure 4.10-17)
- Risk Mitigation Waterfall Schedule (Figure 4.10-18)

It is recommended that a risk-mitigation plan be evaluated to determine its effectiveness. This analysis is performed in the same manner as initial analysis for the risk. The set of templates used for analysis of the risk may also be used to determine the mitigation in the risk level following the completion of each major action or group of actions. The regular reassessment of the risk and performance to plan using a fixed set of criteria provides a consistent analysis of the impact to the program.

The Risk Worksheet (Figure 4.10-7) guides the team through the first three tasks in the Risk Management process: Identify, Analyze, and Develop mitigation planning to obtain a risk reduction decision. When a risk-mitigation plan has been prepared, (Program) Management reviews and approves it based on criteria defined in the Risk Management Plan. The decision is reflected in the disposition blocks at the bottom of the Risk worksheet.

4.10.3.4 Task 4: Implement Risk-Mitigation Plan *(Satisfies iCMM BP 13.05 criteria)*

Once risk-mitigation actions are decided, they shall be implemented and carried out effectively so that either risk likelihood or consequence, or both, are reduced to an acceptable level. The implementation of risk-mitigation actions requires that specific tasks be incorporated into the planning, scheduling, budgeting, and cost-accounting systems used on the program. Incorporating risk-mitigation actions directly into the overall program schedule at a point where risk likelihood or consequence may be affected before a risk occurs keeps management and the

program team aware of the need to allocate resources (labor, materials, and possibly other resources) to accomplish risk-mitigation tasks. The Risk Mitigation Plan Summary chart (Figure 4.10-16) is used as a means of reporting progress in mitigating risks. Each major event in the mitigation plan is identified along with how that event mitigates the risk and to what level.

Incorporating the risk-mitigation plans and milestones into these program processes and systems ensures that the risk and its mitigation plans may be monitored and tracked until the risk is eliminated or the risk requires program modification. Risk-mitigation plans may be documented starting with the Risk Worksheet shown in Figure 4.10-7 and a Risk Mitigation Waterfall Schedule shown in Figure 4.10-18. All mitigation activities are shared with and communicated to all stakeholders.

4.10.3.5 Task 5: Monitor and Track Risks *(Satisfies iCMM PA 14 criteria)*

Reassessing currently managed risks is done on a periodic and event basis to reflect current status of the risks as well as to identify and quantify new and emerging risks. New potential risks to the program may be identified at any time. Newly identified risks are analyzed using the same steps described in Section 4.10.3.2. See risk summary in Figure 4.9-19.

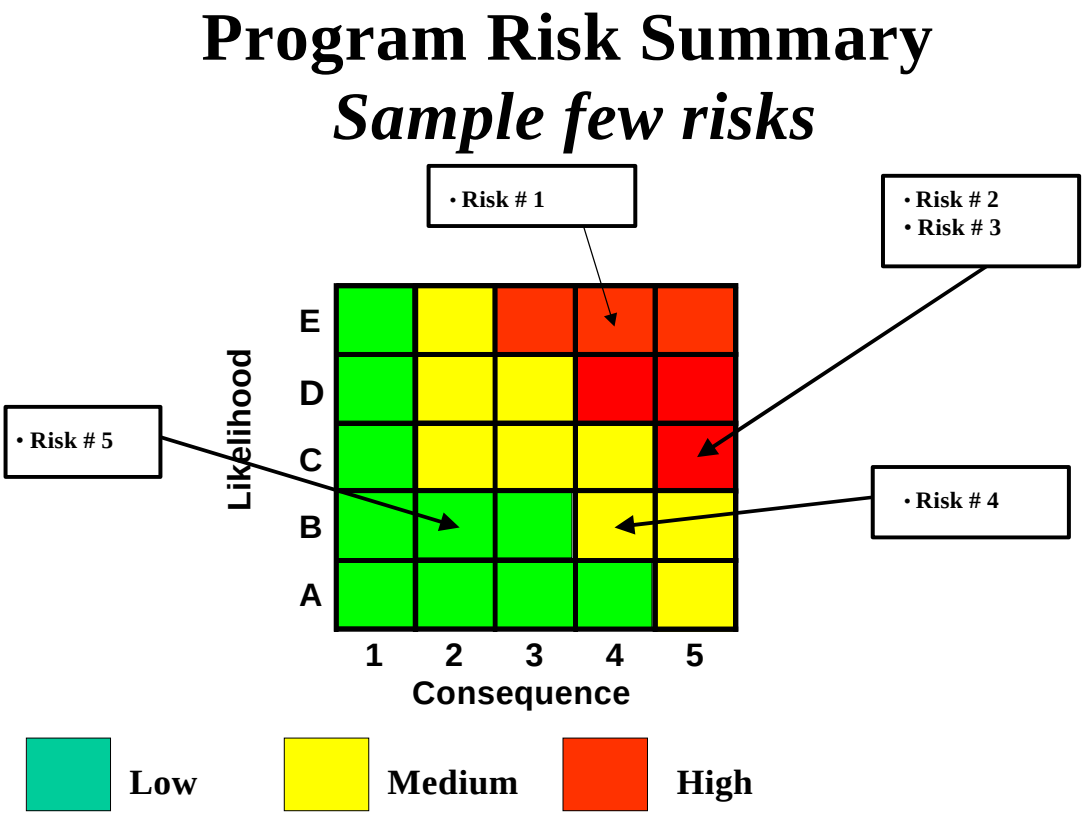


Figure 4.10-19. Program Risk Summary

Steps in the risk-tracking process focus on providing the execution teams, interdependent activities, and program management with program risk trends and status. Actual performance of the planned mitigation actions is compared to the expected performance. The bold line on the Risk Mitigation Plan Summary "waterfall area" (see Figure 4.10-18) indicates progress made

to date on the mitigation plan. Detailed cost and schedule tracking is done as part of the program schedule and cost-tracking system. It is recommended that the Risk Management plan contain the management visibility requirements for the program. These requirements include reporting frequency and content. A sample of a brief summary of all risks for a particular program (or team) with relatively few risks appears in Figures 4.10-19. A standard reporting format shall be used (see Figure 4.10-20) to facilitate integration of risk information across projects and programs. It is recommended that the risk-management plan also indicate the extent of supporting detail, usually in the format of templates (see Figure 4.10-21).

It is recommended that the management visibility effort be focused on monitoring and tracking the effectiveness of the risk-reduction decision. The impact of the risk on program and the relevant ***decision*** are incorporated into the project schedule as risk-mitigation actions. They are inserted into the program's Integrated Program Schedule (Figure 4.10-22). The lowest-level tasks involved are flagged with the assessed risk level; higher-level Work Breakdown Structure tasks inherit the maximum risk level present in any subordinate task. Hence, review of the schedule at any level from

(Extracted from PMR TEMPLATE)

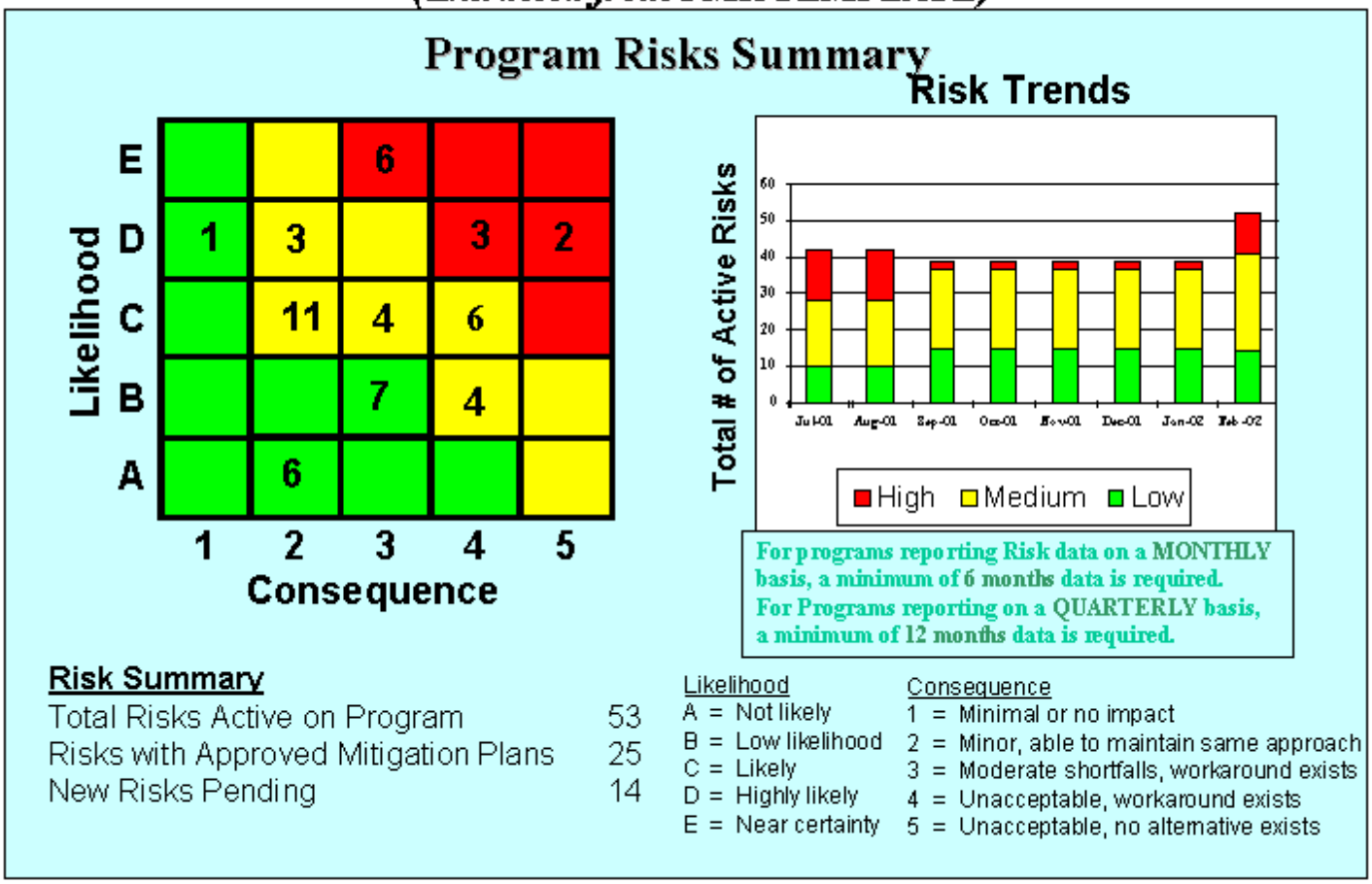


Figure 4.10-20. Standard Risk Reporting Format

(Extracted from PMR TEMPLATES) Program Risks

Risk Level	Risk #	Likelihood	Consequence	Risk Type	Risk	Mitigation	Risk Mitigation Decision Date
H	46	E	4		TSOs and ACs may be delayed Standards	PT will work with industry to secure	Jan-01
H ▶	1	D	5	C	Airspace User Coordination - GA Aircraft users do not accept NEXCOM plan - Benefits for GA not sufficient to engender support - Low end GA	PT reps will meet with reps of the GA community to determine concerns and strategies for resolution of	Jun-02
H ▲	3	D	5	C	Business case does not demonstrate ROI for airlines to equip	PT will establish joint working group with industry to develop business case that industry can support	Jul-02

List risk updates IN PROGRAM PRIORITY ORDER for each New, High Risk item (Red), and Significant Level Changes (High to Low &/or Low to High).

Likelihood
E = Near certainty
D = Highly likely
C = Likely
B = Low likelihood
A = Not likely

Consequence
1 = Minimal or no impact
2 = Minor, able to maintain same approach
3 = Moderate shortfalls, workaround exists
4 = Unacceptable, workaround exists
5 = Unacceptable, no alternative exists

Risk Level:
H - High **M** - Medium **L** - Low
→ = same as last report
↓ = down from last report
↑ = up from last report

Risk Type
T = Technical
S = Schedule
C = Cost

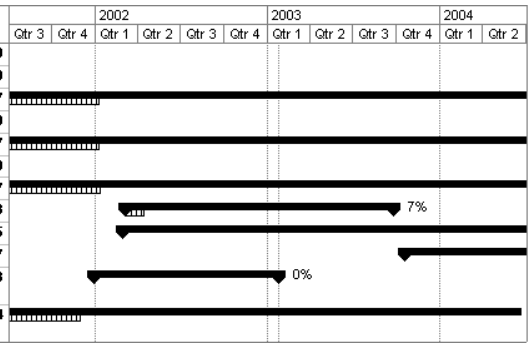
Note: There is a difference between a risk and an issue. If something is a certainty, it is no longer a risk and should be described as an issue and reported on the issues/concerns slide

Initially each High risk should be briefed. Subsequently, any new or major change to a risk item should be captured on this slide. See attached proposed "Risk Management" (Attachment #1) for guidance on how to assess and report program risks.

Figure 4.10-21. Template Formats

Integrated Program Schedule: summary level (top) and "drill-down" to lowest level tasks (bottom).

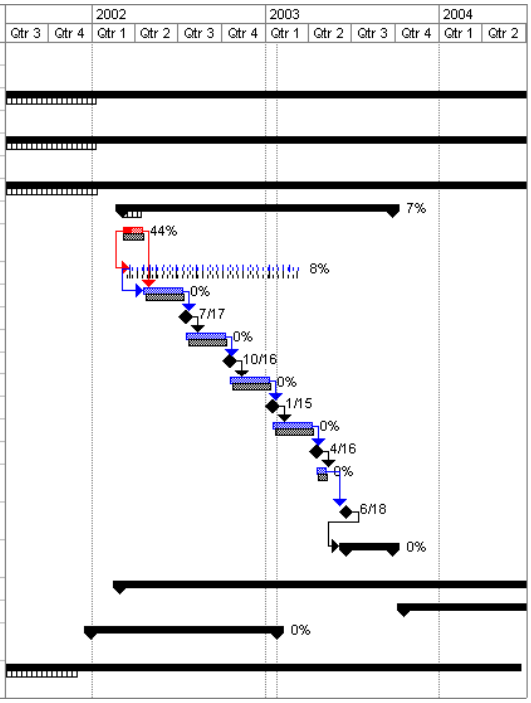
ID	Task Name	Risk	Start	Finish
1	**Mission Analysis**		**10/1/99**	**10/5/99**
7	**Investment Analysis**		**10/6/99**	**10/11/99**
17	**Solution Development**		**10/11/99**	**3/22/07**
18	**Program management**		**10/12/99**	**10/12/99**
22	**System Engineering**		**10/11/99**	**1/23/07**
23	**System Requirements and Definition**		**10/13/99**	**10/13/99**
25	**Analysis, Design, and Integration**		**5/31/01**	**1/23/07**
26	**Enhanced Visual Approach - Level 1**		**3/6/02**	**9/24/03**
44	**CDTI-Enhanced Flight Rules - Level 2**		**2/28/02**	**1/7/05**
70	**CDTI-Enhanced Flight Rules - Level 3**		**10/20/03**	**1/23/07**
96	**Terminal Area Multilateration Performance Evaluation**		**12/31/01**	**1/24/03**
113	**Terminal Area Common ARTS Integration**		**5/31/01**	**6/21/04**



Risk information displayed at summary task level in the program Integrated Master Schedule (IMS)

High risk
Medium risk
Low risk

ID	Task Name	Risk	Start	Finish
1	**Mission Analysis**		**10/1/99**	**10/5/99**
7	**Investment Analysis**		**10/6/99**	**10/11/99**
17	**Solution Development**		**10/11/99**	**3/22/07**
18	**Program management**		**10/12/99**	**10/12/99**
22	**System Engineering**		**10/11/99**	**1/23/07**
23	**System Requirements and Definition**		**10/13/99**	**10/13/99**
25	**Analysis, Design, and Integration**		**5/31/01**	**1/23/07**
26	**Enhanced Visual Approach - Level 1**		**3/6/02**	**9/24/03**
27	*Resolve concerns with data collection procedures*		3/6/02	4/17/02
28	*Carrier #1 equipage*		3/20/02	3/20/03
29	Data collection period #1		4/17/02	7/10/02
30	Metrics report #1		7/17/02	7/17/02
31	Data collection period #2		7/17/02	10/9/02
32	Metrics report #2		10/16/02	10/16/02
33	Data collection period #3		10/16/02	1/8/03
34	Metrics report #3		1/15/03	1/15/03
35	Data collection period #4		1/15/03	4/9/03
36	Metrics report #4		4/16/03	4/16/03
37	*Document 1% - 3% improvement in terminal arrival rat*		4/16/03	5/7/03
38	Decision Point - Does data support Level 1 equippage?		6/18/03	6/18/03
39	**Certify CDTI use during visual approach**		**6/18/03**	**9/24/03**
44	**CDTI-Enhanced Flight Rules - Level 2**		**2/28/02**	**1/7/05**
70	**CDTI-Enhanced Flight Rules - Level 3**		**10/20/03**	**1/23/07**
96	**Terminal Area Multilateration Performance Evaluation**		**12/31/01**	**1/24/03**
113	**Terminal Area Common ARTS Integration**		**5/31/01**	**6/21/04**



"Drill-down" capability - Risk information displayed for lowest level tasks; summary tasks show highest level of risk for any subordinate task

Figure 4.10-22. Risk Information Incorporated Into Program

summary tasks (Figure 4.10-22, top) to lowest-level tasks (Figure 4.10-22, bottom) allows program management to maintain appropriate risk visibility, and also allows "drill-down" to increasing levels of detail as the schedule view is expanded.

Effective program management always involves examining cost and schedule during review of the progress of the program. Making risk information visible as part of the IMS ensures that risk

information receives ongoing management attention. Integrating program risk data into the integrated master schedule fosters better, risk-based decisionmaking in at least three ways:

- The need for separate risk reviews competing for the program manager's time and energy is eliminated.

- Integrating the risk information into the IMS effectively prevents isolation of the risk efforts from the mainstream tasks and program milestones. The risk profile of the program is presented as part of the overall management view of the program. As each decision point is reached, the risk information associated with that event is portrayed, and hence, shall be considered.

- The portrayal of program progress illustrated in Figure 4.10-22 alerts management to when a decision needs to be made and what that decision is. This provides visibility across the entire program ***in advance*** of impending decision points so that the necessary relevant information is provided in a timely manner to support an informed decision.

4.10.4 Outputs *(Satisfies iCMM Artifacts criteria)*

The five major outputs of this process are:

- Risk-Mitigation Plans (see Section 4.10.3.3)

- Risk Mitigation Plan Summary (Figure 4.10-18)

- Program Risk Mitigation Progress Chart (Figure 4.10-19)

- Program Risk Summary (Figures 4.10-20 and 4.10-21)

- Program Risk Register (Figure 4.10-23)

It is recommended that the Program Risk Summary, the Risk Mitigation Plan Summary, and the Program Risk Mitigation Progress charts be briefed at all regular program reviews. Management decisions are based on the above information. It is recommended that a complete status of a given risk be briefed when the risk is identified and immediately following the risk realization date.

It is recommended that the Risk-Mitigation Plan be considered an appendix to the IPP and Acquisition Program Baseline. It shall be handled as an integral part of program effort.

4.10.5 Risk Management Tools

The tools needed to implement this process include:

- Approved Risk Management Plan

- FAA Risk Worksheet

- Likelihood and consequence templates tailored for the program

- Risk Mitigation Plan Summary
- A means to communicate results across a program (electronic mail, servers, etc.)
- A means to document the results of the process and manage the outputs (databases, spreadsheets, word processors, etc.)
- Analytical tool(s) to support Risk analysis and tracking

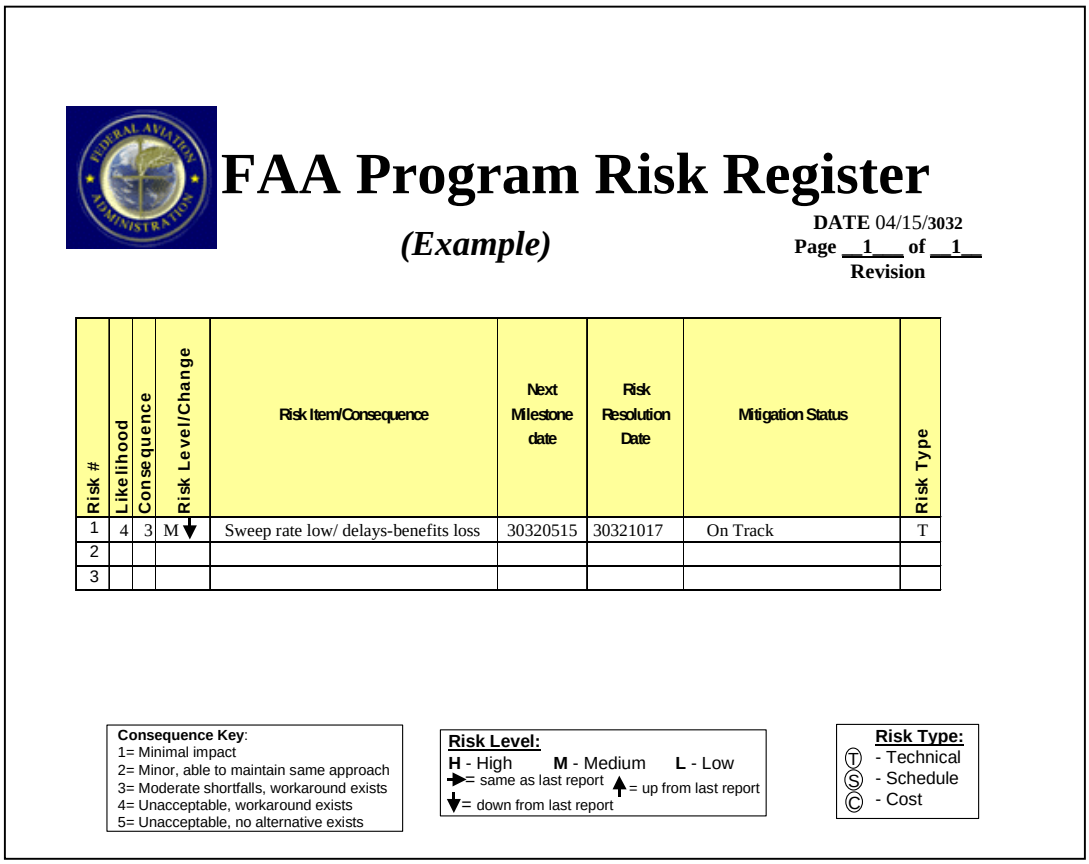
4.10.5.1 Analytical tools

An example of a database tool is “Risk Radar” (a tool free to the government that may be used to generate many of the risk work products (see Section 4.10-7)). A version of Risk Radar that incorporates the FAA templates and forms is available for download (http:TBD). This software is available free to all FAA programs (including contractors for use in supporting FAA programs). It requires MS Access 2000 and interfaces with MS Project 2000 for schedule linkage to the overall Program Master schedule.

Analytic tools may be used for probabilistic analysis of schedule uncertainty or technical uncertainty. Critical Path Analysis tools may be used with the Integrated Program Schedule to regularly evaluate schedule risk. In a similar fashion, commercial applications (e.g., @RISK) may be applied to technical parameters (such as weight, latency, power, computer throughput) to establish confidence ranges. Results from these probabilistic analyses may support the overall risk analysis task of establishing a likelihood of occurrence. Further details on the use of probabilistic analysis appear in textbooks and technical papers that cover statistical analysis for risk management.

4.10.5.2 Risk register

The risk register (see example in Figure 4.10-23) is a listing of risk information associated with achieving program objectives. If risk registers are created and maintained by each project, a single composite register of all interdependency risk items shall be developed for the program. These registers are to be consistently used to monitor and track overall risk status within team meetings, program management reviews, and major program reviews. Immediately following identification and analysis of a new medium or high risk or when a significant change occurs in a previously identified risk, changes shall be incorporated in the register and other documents and the new risk identified to stakeholders. The distribution list is to be established and documented in a program's Risk Management Plan. Computer database systems may be needed to manage these outputs for large programs. Smaller programs may often be able to use desktop computer techniques. At a minimum, the following information shall be included in the risk register:



FAA Program Risk Register

(Example)

DATE 04/15/**3032**
Page __1___ of __1__
Revision

Risk #	Likelihood	Consequence	Risk Level/Change	Risk Item/Consequence	Next Milestone date	Risk Resolution Date	Mitigation Status	Risk Type
1	4	3	M ↓	Sweep rate low/ delays-benefits loss	30320515	30321017	On Track	T
2								
3								

Consequence Key:
1= Minimal impact
2= Minor, able to maintain same approach
3= Moderate shortfalls, workaround exists
4= Unacceptable, workaround exists
5= Unacceptable, no alternative exists

Risk Level:
H - High **M** - Medium **L** - Low
→ = same as last report ↑ = up from last report
↓ = down from last report

Risk Type:
Ⓣ - Technical
Ⓢ - Schedule
Ⓒ - Cost

Figure 4.10-23. Risk Register

4.10.5.2.1 Risk Register Identification and Creation/Update Date

This is the name of the program risk item. Indicate the root cause of the risk in this section.

4.10.5.2.2 Risk Identification Number

This number is code that identifies a unique sequence.

4.10.5.2.3 Likelihood

This is a figure-of-merit indicating the relative likelihood/probability that the identified risk will actually occur (Likelihood Template, Figure 4.10-9).

4.10.5.2.4 Consequence

This is a figure-of-merit indicating the relative severity of consequences/impacts that could result if the identified risk did occur (Consequences Templates, Figures 4.10-10, 4.10-11, and 4.10-12, for examples).

4.10.5.2.5 Risk Level/Change

This is a single letter indicating the assessed risk of an item as high, medium, or low (H, M, L) or, red, yellow, or green (R, Y, G), respectively. An arrow that indicates the direction that the risk has moved since the last revision to the risk register demonstrates the risk change.

4.10.5.2.6 Risk Consequence Description

This is a brief, well-stated description of the risk's negative consequences.

4.10.5.2.7 Next Milestone Date

This date is the projected date at which the risk level converts to lower risk. This is traceable to the Risk Mitigation Plan Summary (See Figure 4.10-17).

4.10.5.2.8 Risk Realization Date

This is the date (or point in time) of the event that either makes the risk a real part of the program or eliminates the need to track the risk. Early in the program, it may be difficult to predict an exact date, but a general timeframe needs to be developed. As the program matures, date realization occurs. It is recommended that these dates be reviewed regularly and be on the program master schedule.

4.10.5.2.9 Mitigation Status

The currently planned mitigation actions are defined.

4.10.5.2.10 Risk Type

The risk type designates if the risk is a cost risk, a schedule risk, or a technical risk (see Paragraph 4.10.3.1.1).

4.10.5.2.11 Risk-Mitigation Plan Status

The teams regularly update and report the status of the risk-mitigation plan for each risk being tracked that requires risk handling. Actions are initiated as required in which mitigation plan activities are not being accomplished. The risk status is also reviewed with program management on a regular basis. A sample of a brief summary of all risks for a particular program (or team) is shown in a Program Risk Summary (Figures 4.10-19 and 4.10-20) for use depending on program size.

4.10.6 Risk Management Process Metrics *(Satisfies iCMM PA 18 criteria)*

It is recommended that Risk Management-related metrics be focused on Program and/or Project success criteria. At the Program level these metrics measure program progress to plan. Earned Value Management is an excellent set of measures to portray the extent of schedule and cost risk in a program. The variance to plan for either Schedule Performance Index or Cost Performance Index may be used as a measure of risk on the Program. Technical or performance risk may be measured through by using Technical Performance Measures. The projected and/or actual variance to performance requirements is a measure of technical risk. At a lower level, metrics for the Risk Management process itself may include:

- **Total risks identified over time; total high risks, total medium risks.** The objective is to provide visibility into risk trends over time.

- **Percent of risks (medium and high) with approved mitigation plans.** The objective is to measure the effectiveness of handling the risks requiring action.

- **Percent of overdue mitigation activities.** The objective is to measure the effectiveness of meeting mitigation plan schedules.

- **Aging of active risk records.** The objective is to gain insight into the currency of the risk database.

- **Number of risks past their realization date.** The objective is to provide an indicator of the effectiveness to handle risks in a timely manner.

Major FAA programs are required to submit yearly budget estimates with supporting justification for the investment in accordance with Office of Management and Budget (OMB) Circular A-11 (Ref 22). These submissions are provided as an "Exhibit 300" in a format proscribed by OMB. OMB uses risk as a factor to measure the health of investment programs based on the Exhibit 300 data. The OMB scoring criteria for Risk Management is shown in Figure 4.10-24. OMB requires that the risk related data be presented in 19 categories defined in Circular A-11. The OMB requirement is for reporting purposes to provide OMB objective evidence that all aspects of risk have been considered in managing FAA investments. Figure 4.10-25 provides a crosswalk between the Investment Analysis process used in support of the FAA Investment decision(s) that evaluates the source(s) of risk for each investment alternative, risk implementation categories discussed in the SEM that are used for the ongoing management of programs and organizations, and the OMB reporting categories used by OMB to gauge the health of our investment programs.

OMB Exhibit 300 – Business Case Scoring

Risk Management

5: Risk Assessment was performed for all mandatory elements and risk is managed throughout the project.

4: Risk assessment addresses some of the risk, but not all that should be addressed for this project.

3: Risk Management is very weak and does not seem to address or manage most of the risk associated with the project.

2: Risk Assessment was performed at the outset of the project but does not seem to be part of program management.

1: There is no evidence of a Risk Assessment Plan or Strategy.

Scoring Element	Score
Risk Management (RM)	
Performance Goals (PG)	
Security (SE)	
Performance Based Management System (PB)	
Life Cycle Costs Formulation (LC)	

Figure 4.10-24. OMB Risk Scoring Criteria

Risk Reporting Throughout the System Lifecycle

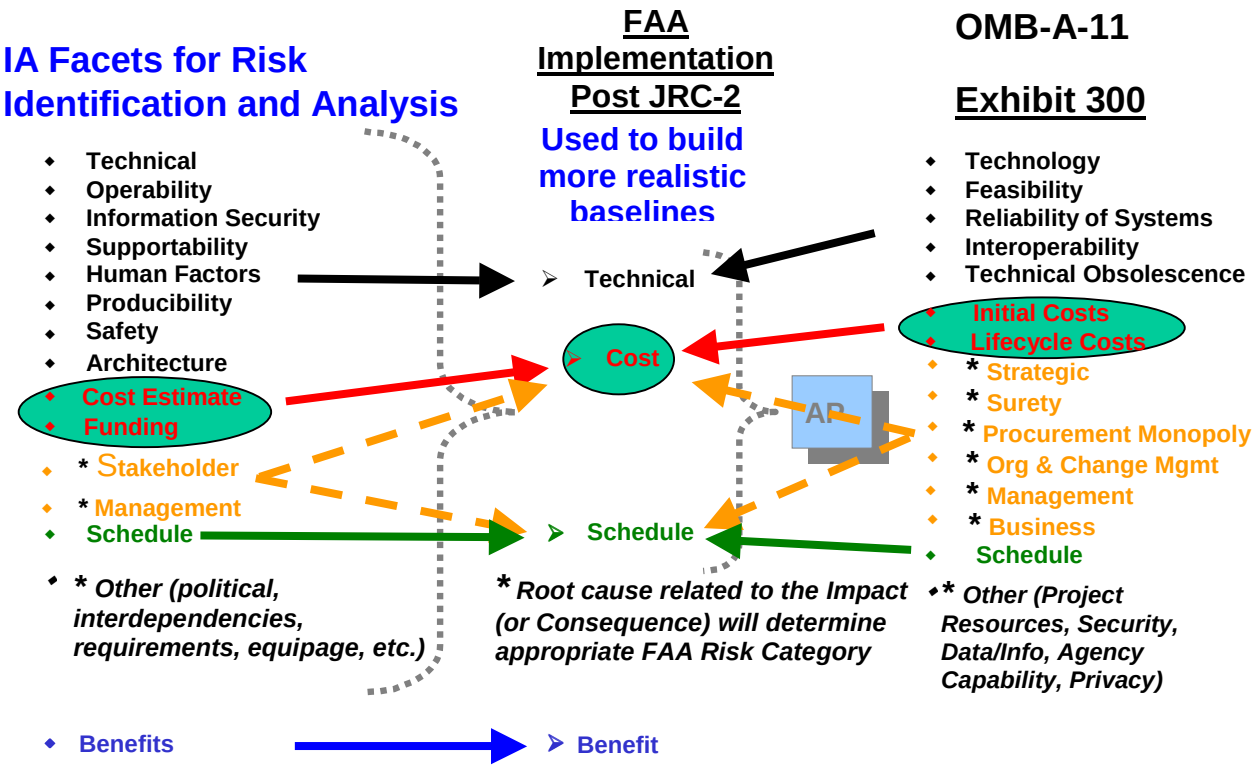


Figure 4.10-25. Risk-Reporting Crosswalk

4.10.7 References

1. U.S. Air Force, Air Force Materiel Command. *Risk Management.* Pamphlet 63101. AFMC, 09 July 1997. http://www.sm.nps.navy.mil/mn3331_core/Calendar/Week6/Readings6/Risk_Mgt/USAF_Risk Mgmt_Guide.doc

2. American National Standards Institute/Electronic Industries Alliance. *Processes for Engineering a System*. ANSI/EIA-632-1998, pp. 11, 13, 14, 17, 30, 33-4, 45, 49, 52, 67, 75, 77, 81, 96, 109. Requirement 24.

3. Blanchard, Benjamin S., and Walter J. Fabrycky. *Systems Engineering and Analysis.* Third edition. Englewood Cliffs, NJ: Prentice Hall, 1998, pp. 657-661.

4. Conrow, Edmund H. *Effective Risk Management.* Reston, VA: American Institute of Aeronautics and Astronautics, Inc., 2000. http://www.risk-services.com/aiaabok1.htm.

5. Department of Defense. *Transition from Development to Production.* DOD 4245.7-M. Chapter 9-8. Washington, DC: U.S. Department of Defense, September 1985.

6. U.S. Department of Transportation. *Departmental Guide to Risk Management Planning.* DOT H 1350.252. Washington, DC: U.S. Department of Transportation, 22 May 1999.

7. Defense Acquisition University Press. *Risk Management Guide for DoD Acquisitions.* Fifth edition. Fort Belvoir, VA: Defense Acquisition University Press, June 2002. http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm

8. Defense Systems Management College. *Systems Engineering Management Guide*. Chapter 15. Fort Belvoir, VA: Defense Systems Management College, 1990.

9. Electronics Industries Alliance. *Processes for Engineering a System*. EIA 632. Arlington, VA: Electronics Industries Alliance, January 1999. 08/09/02. Rev. 99, Chg.H. http://www.eia.org

10. Federal Aviation Administration. *FAA Acquisition Management System*. Paragraph 2.9.14. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. http://fast.faa.gov/.

11. Federal Aviation Administration. *FAA Acquisition Program Baseline Template*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. http://fast.faa.gov.

12. Federal Aviation Administration. *FAA Orders 1900.47, 1050, 1600, 3900, and 1370.82.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.

13. Federal Aviation Administration. *Acquisition and Program Risk Management Guidance.* FAA P1810. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 1996.

14. Federal Aviation Administration. *Risk Assessment Guidelines for the Investment Analysis Process.* FAA Working Paper No. WP-59-FA7N1-97-2. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 1999.

15. Accounting and Information Management Division. *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making.* GAO/AIMD-10.1.13. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, February 1997, Section 10.1.13.

16. Accounting and Information Management Division. *Information Security Risk Assessment.* GAO/AIMD-99-139. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, August 1999.

17. U.S. General Accounting Office. *Determining Performance and Accountability Challenges and High Risks, Exposure.* Draft. GAO/OCG-00-12. Washington, DC: U.S. General Accounting Office, August 2000.

18. Grady, Jeffery O. *Systems Requirements Analysis*. New York, NY: McGraw-Hill, 1993, pp. 462-465. http://www.mcgraw-hill.com/

19. Grady, Jeffery O. *System Engineering Planning and Enterprise Identity*. Boca Raton, FL: CRC Press, 1995, pp. 168-177.

20. Grady, Jeffery O. *System Integration.* Boca Raton, FL: CC Press, 1994, p. 149.

21. Shish, Robert. *NASA Systems Engineering Handbook.* NASA SP-6105. Washington, DC: National Aeronautics and Space Administration, June 1995, pp. 37-44.

22. Office of Management and Budget. *Planning, Budgeting, Acquisition, and Management of Capital Assets.* OMB Circular No A-11, Part 7. Washington, DC: Office of Management and Budget, June 2003.

23. Project Management Institute. *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide 2000 Edition). Chapter 11. Newton Square, Pennsylvania.

24. Ross, John F. *Living Dangerously: Navigating the Risks of Everyday Life.* Cambridge, MA: Perseus Publishing, 1999. http://www.questia.com/PM.qst?action=openPageViewer&docId=85921102.

25. *Best Practices: How to Avoid Surprises in the World's Most Complicated Technical Process —The Transition from Development to Production*. DON NAVSO P-6071, March 1986.